IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

KRISTEN RUELL, *Plaintiff* v. **DENIS R. MCDONOUGH, SECRETARY DEPARTMENT OF VETERANS AFFAIRS,** *Defendant*	**Case No. 2:23-cv-03513-JDW**

MEMORANDUM

The U.S. Department of Veterans Affairs set up a case and correspondence management tool that provided inadequate protections for sensitive information. Kristen Ruell works at the VA and, as a whistleblower, had information in the documents in that system. Because the VA's system fell short, other VA employees could potentially view her information, and she posits that they did. She seeks to hold the VA liable as a result.

Ms. Ruell's claims fail for three reasons. She didn't exhaust her administrative remedies, so she can't prevail on her claims for injunctive relief. She hasn't shown that the VA acted willfully or intentionally, so she can't prevail on her damages claims. Her remaining claims, under the criminal provisions of the Privacy Act, the Inspector General Act of 1978 ("IGA"), and the Veterans Benefits, Health Care, and Information Technology Act of 2006 ("VBHCITA") fail because none of those provisions offers a private right of action.

I. BACKGROUND

A. VIEWS

The VA utilizes a Case and Correspondence Management ("CCM") system for official VA correspondence. The VA's Integrated Enterprise Workflow Solution ("VIEWS") is a Salesforce tool that the VA uses as part of its CCM. Since 2018, the VA has used VIEWS to access, maintain, and process documents in CCM. Only trained, supervisor-approved VA employees can use the VIEWS software tool. Since 2018, the VA has authorized approximately 0.5% of its employees to access VIEWS. As of July 2024, about 2,015 VA employees had authorization to access the VIEWS system.

When a user initiates a case in VIEWS, the user must select a "case sensitivity" level for the case and all the documents related to it. The case sensitivity level options are: "sensitive," "not sensitive," and "pending." (ECF No. 37-2 ¶ 21.) When a user marks a case "sensitive," only the team assigned to work on the case can access the case and its corresponding documents. A user should mark a case "sensitive" when it contains personally identifiable information ("PII") or sensitive personal information ("SPI"), such as names, home addresses, phone numbers, social security numbers, and dates of birth, or when it contains protected health information ("PHI").

From 2018 until August 2022, the VA used a security tool called Salesforce Shield to track each time a user accessed a case or downloaded a document in VIEWS, known as "security event logs." (ECF No. 37-10 ¶ 8.) Before then, "there was no capability to track who

accessed a particular document or case file" in the VA's prior system of records." (ECF No. 37-10 ¶ 7.) The VA maintains different types of security events. "Case Access" means a user has searched VIEWS and then "accessed" a case by engaging with the case's content, like clicking on a document. "Web Clicks" means that a user has "accessed" a case through means other than a VIEWS search, such as clicking on a VIEWS link. "Document views/Downloads" means that a user downloaded a document associated with a case. The system does not generate a security event just based on a search that someone runs or a view of a case or the records attached to a case, so security event logs do not capture those actions. Per the VA's security retention policies, Salesforce Shield retained security event logs for a maximum of 30 days. Thus, most security event logs from before August 2022 no longer exist.

In August 2022, the VA replaced Salesforce Shield with Splunk, a Security Information and Event Monitoring tool. Only VA system administration and IT security professionals can use Splunk. Thus, average VIEWS users cannot use Splunk to create security event logs for individual cases. Splunk can retain security event logs for a minimum of one year and up to six years, and the VA has retained all security event logs since Splunk's implementation in August 2022. Thus, one can search the Splunk logs from August 2022 through the present. Some security event logs from June and July 2022 are also available.

B. SORN

Pursuant to the Privacy Act, the VA published a System of Records Notice ("SORN") in the Federal Register, advising that:

> The … [CCM] is the Secretary's official correspondence record, and includes the name, address and other identifying information pertaining to the correspondent, as well as background information concerning matters which the correspondent has brought to the Department's attention. The system of records also contains documents generated within VA that may contain the names, addresses and other identifying information of individuals who conduct business with VA, as well as material received, background information compiled and/or response sent.

SORN at 36584.[1] The notice makes clear that the VA keeps paper records and maintains electronic records in VIEWS. SORN explains that the VA keeps the "[f]ull name, postal address, email address, phone and fax numbers of individuals corresponding with the Department, … as well as supporting documents." *Id.* at 36585. And "[r]ecords are retrieved using name, claim file number, **social security number**, date of birth, and other unique identifiers belonging to the individual to whom the information pertains." *Id.* at 36586 (emphasis added).

For individuals "seeking information on the existence and content of records" pertaining to them, they "should contact the system manager [(Uriel Williams)] in writing …." *Id.* "A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort." *Id.* Individuals "seeking to contest or amend records" in the VA's system must also contact Mr. Williams in writing, and any "request to contest or amend records must state clearly and

[1] All citations to SORN refer to 87 FR 36584-01.

concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record." *Id.*

C. Ms. Ruell's Records

Ms. Ruell has worked for the VA since 2007. She is not an approved VIEWS user and has never had access to VIEWS. In 2014 and 2015, she testified as a whistleblower before the United States Congress regarding system errors that impacted veterans' benefit payments. As a whistleblower, Ms. Ruell alleges that she communicated with members of Congress, White House officials, the VA Secretary and other VA officials, and media outlets. Some of her confidential whistleblower communications are stored in VIEWS and contain her PII and SPI. In addition, some of Ms. Ruell's PII appears in other individuals' records in VIEWS because she assisted other VA employees when they filed administrative claims against the VA.

On June 23, 2022, another VA employee and whistleblower, Peter Rizzo,[2] searched for his own name in VIEWS and viewed documents that contained his whistleblower communications with a congressional representative. Mr. Rizzo and Ms. Ruell know each other, and Mr. Rizzo knew that Ms. Ruell was also a VA whistleblower. Mr. Rizzo searched for Ms. Ruell's name and accessed documents pertaining to her that no one had marked sensitive. Mr. Rizzo was not assigned to work on any of Ms. Ruell's cases in VIEWS. However, he downloaded the documents and saved them locally to his VA laptop. Ms.

[2] Mr. Rizzo no longer works for the VA.

Ruell did not give Mr. Rizzo permission to view or download documents pertaining to her. Mr. Rizzo called Ms. Ruell and told her that he could access documents pertaining to her in VIEWS. During a virtual meeting, Mr. Rizzo shared his screen so that Ms. Ruell could see the documents that were accessible in VIEWS. Ms. Ruell asked Mr. Rizzo to send her whatever documents he found when he searched her name in VIEWS, and he sent her 76 case files. The documents contained Ms. Ruell's whistleblower communications and PII.

In July 2022, Mr. Rizzo and Ms. Ruell reported their findings to a woman named Maureen Elias.[3] In an email, Ms. Ruell asked Ms. Elias for "the plan to protect" her information and reported that it was "concerning to me knowing that thousands of users can view my confidential whistleblower communications and my Pii …." (ECF No. 1-1 at 122 of 126.) Ms. Ruell wrote back to Ms. Elias the following month and expressed concern that her PII was "still not marked sensitive in VIEWS." (*Id.* at 119 of 126.) At some point, Ms. Ruell reached out to Rita Grewal, Branch Chief, VA Privacy Risk Management & Compliance, about her concerns. In May 2023, Ms. Ruell wrote a follow-up email to Ms. Grewal and explained that she had "concerns with the information being unsecured, not marked sensitive[.]" (ECF No. 40-1 at 2.)

Ms. Ruell never contacted the VA's system manager, Uriel Williams, to request access to her records in VIEWS or to amend them. Instead, in 2022, she "went to the top" and "basically contacted the VA Chief of Staff" to report that her whistleblower

[3] The record does not identify Ms. Elias or make clear what her role was at the VA.

communications and PII were not marked sensitive in VIEWS. (ECF No. 46-1 at 261:10-16.) She and Mr. Rizzo also contacted the VA Office of Special Counsel ("OSC"), the VA Inspector General, Deputy Chief of Staff at the VA, and the House and Senate Veterans Committees to report that they believed that certain documents in VIEWS should be marked sensitive but were not.

On August 2, 2022, OSC requested that the VA investigate Ms. Ruell's allegations, along with security complaints received by other employees. VA Investigator John Scott led the investigation. The VA investigated the allegations and completed a draft report on July 21, 2023 ("VA Report"). The VA Report noted that "VIEWS CCM has an integrated logging capability that displays changes made to case information and changes made by users, but it does not capture instances where a user simply viewed case information or downloaded files." (ECF No. 42-6 at 14.) The VA Report reasoned that "in light of this auditing limitation, it is unclear how business and system owners are able to accomplish risk mitigations in the form of auditing user activity …." (*Id.*)

In addition, the VA Report acknowledged that many cases in the VIEWS system "had been incorrectly designated as 'Not-Sensitive,'" meaning that any active VIEWS user could "view, download, copy, screenshot, or otherwise share sensitive information - e.g., whistleblower and Veteran social security numbers, dates of birth, home addresses and phone numbers, and medical and financial information—without a need-to-know, and without the authorization or knowledge of business and system owners." (*Id.* at 8.) While

the VA could not determine the exact number of improperly-designated cases that contained whistleblower information and other SPI, it "easily estimated" the number of such cases "to have been in the multi-thousands" at the time Ms. Ruell and other whistleblowers came forward with their allegations. (*Id.*)

The VA Report noted that "VA officials still need to take additional measures to protect the confidentiality of whistleblower identities, their submissions, and PII in VIEWS CCM" and included specific recommendations for the VA to improve and remediate these security concerns. (*Id.* at pg. ii.) The Report also emphasized that "there is no evidence that VIEWS vulnerabilities discussed in this report resulted in a privacy breach or has caused harm to Veterans, whistleblowers, or their families." (*Id.* at pg. iii.) The VA implemented corrective actions following the report, and the OSC reported the matter closed as of September 3, 2024.

During the VA's investigation into Ms. Ruell's and others' complaints about VIEWS, Ms. Ruell continued to express concern that the VA had not marked her records "sensitive." In June 2023, Ms. Ruell asked a former colleague, Ken Olivo, to search for her name in VIEWS and "see if anything comes up." (ECF No. 46-1 at 33:20-21.) Mr. Olivo was an authorized VIEWS user, but the VA never assigned him to work on any of Ms. Ruell's cases. Mr. Olivo confirmed with Ms. Ruell that when he searched her name in VIEWS "everything came up that's not supposed to" and that the VA had not marked the documents "sensitive." (*Id.* at 33:22-24.) Wanting to verify this, Ms. Ruell asked the VA's

internal investigator, Mr. Scott, to confirm whether he could view the documents. Mr. Scott confirmed that there were "at least 12 documents" in VIEWS that contained Ms. Ruell's PII but were not marked "sensitive." (*Id.* at 34:13.)

After Ms. Ruell shared this information, Mr. Williams, Data Manger for the VA Office of the Executive Secretary, System Manager for CCM, and VIEWS VA Product Owner, marked all her records in VIEWS as "sensitive." He has attested that all of Ms. Ruell's records in VIEWS have remained "sensitive" since then. He also removed all the case team members assigned to her records, so that he is the sole member of her case team. As a result, Mr. Williams stated that "as of June 16, 2023, Ms. Ruell's records are visible only to [Mr. Williams] as her sole case team member; Dan Navarra, as an IT superuser, and the [VA's Digital Transformation Center ("DTC")] security team responsible for generating security event logs upon request." (ECF No. 37-2 ¶ 14.) However, following another request from Ms. Ruell on July 25, 2023, Mr. Olivo confirmed that he was ***still*** able to access her case files and that "all Congressional correspondence and legal reviews" and other documents were "accessible [to him] for view/download …." (ECF No. 42-5 at 2.) In addition, on August 9, 2023, Mr. Scott confirmed that her "whistleblower communications and pii are ***still viewable*** to all users." (ECF No. 42-7 at 2 (emphasis added).)

Neither Ms. Ruell nor the VA knows if anyone viewed or accessed Ms. Ruell's records before June 2022 because Salesforce Shield only retained security event logs for 30 days. Since then, there is evidence that at least 14 different VIEWS users accessed one

of Ms. Ruell's cases by running a search or through a web click. However, neither the VA nor Ms. Ruell knows if any of those users viewed any of her records. In addition, there is evidence that nine individuals (including Mr. Rizzo) downloaded documents pertaining to Ms. Ruell. Coupled with the evidence that Mr. Olivo viewed her records on two occasions in June 2023, there is evidence that at least 10 people have viewed Ms. Ruell's records since June 23, 2022. Aside from Messrs. Rizzo and Olivo, "everyone who 'accessed' or downloaded Ms. Ruell's documents from June 2022 through the present … is either on Ms. Ruell's case team; was tasked with marking her documents sensitive; is an attorney within VA OGC; was assigned to conduct an internal investigation into Ms. Ruell's complaint on behalf of [the Office of Information Technology ("OIT")]; or is a member of the DTC Security Admin Team tasked with generating the security event log reports" that the VA submitted as part of its summary judgment briefing. (ECF No. 37-15 ¶ 4.)

Ms. Ruell does not claim to have suffered any harm from Messrs. Rizzo and Olivo viewing her records in VIEWS. Instead, she contends that over the past 11 years, "[m]oney was taken from [her] Wells Fargo Bank account," which she attributes to the VA's "publication of [her] sensitive and personally identifiable information." (ECF No. 40 at 14.) As a result, Ms. Ruell purchased Norton LifeLock identity theft monitoring software. She also contends that as result of the alleged disclosure of her records, the VA retracted a detail opportunity and that she has suffered from "emotional distress and reputational harm, loss of wages, loss of leave, vandalism to her car, doxing, etc." (*Id.* at 20.)

D. Procedural History

On September 10, 2023, proceeding *pro se*, Ms. Ruell filed suit against the Secretary of the VA, Denis McDonough.[4] She filed an Amended Complaint alleging various violations of the Privacy Act of 1974. The first two causes of action seek injunctive relief, the third and fourth claims seek damages, and the fifth and sixth seek to enforce criminal penalties under Privacy Act. She also asserts violations of the IGA (Seventh Cause of Action) and the VBHCITA (Eighth Cause of Action). She seeks declaratory relief pursuant to the Declaratory Judgment Act.[5] The VA moved for summary judgment on all of Ms. Ruell's claims, and the motion is ripe.

II. LEGAL STANDARD

Federal Rule of Civil Procedure 56(a) permits a party to seek, and a court to enter, summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). In ruling on a summary judgment motion, a court must "view the facts and draw reasonable inferences 'in the light most favorable to the party opposing the [summary

---

[4] The Privacy Act authorizes civil suits against federal agencies, not individuals. *See* 5 U.S.C. § 552a(g)(1). Thus, a plaintiff cannot assert claims against individual employees of an agency. *See Martinez v. Bureau of Prisons*, 444 F.3d 620, 624 (D.C. Cir. 2006). Because Ms. Ruell is proceeding *pro se*, the VA has construed her claims as asserted against the agency itself, rather than Secretary McDonough, who Ms. Ruell named as a Defendant. Ms. Ruell has not objected to that approach, so I will do the same.

[5] In her opposition brief, Ms. Ruell confirmed that she is ***not*** pursuing a claim under the Whistleblower Protection Act in the present litigation. (*See* ECF No. 40 at 17.)

judgment] motion.'" *Scott v. Harris*, 550 U.S. 372, 378 (2007) (quotation omitted). "The non-moving party may not merely deny the allegations in the moving party's pleadings; instead, [s]he must show where in the record there exists a genuine dispute over a material fact." *Doe v. Abington Friends Sch.*, 480 F.3d 252, 256 (3d Cir. 2007) (citation omitted); *see also* Fed. R. Civ. P. 56(c)(1)(A)-(B). If she fails to make this showing, then the court may "consider the fact undisputed for purposes of the motion" and/or "grant summary judgment if the motion and supporting materials — including the facts considered undisputed — show that the movant is entitled to it[.]" Fed. R. Civ. P. 56(e)(2), (3).

III. ANALYSIS

A. Privacy Act Claims

1. Injunctive relief claims

The Privacy Act creates a civil right of action based on an agency's "deficient management of records." *Doe v. Chao*, 540 U.S. 614, 618 (2004). In an "amendment" claim under Section 552a(g)(1)(A), the Act "provides for the correction of any inaccurate or otherwise improper material" in an individual's record. *Id.* An "access" claim under Section 552a(g)(1)(B), in contrast, "provides a right of access against any agency refusing to allow an individual to inspect a record kept on [her]." *Id.* For each claim, the act provides for injunctive relief and fees and costs, but not damages. *See* 5 U.S.C. § 552a(g)(2), (3).

Courts require a plaintiff asserting either an amendment claim or an access claim to exhaust her administrative remedies before asserting that claim in court. *See, e.g.,*

Taylor v. U.S. Treasury Dept., 127 F.3d 470, 474 (5th Cir. 1997); *Haase v. Sessions*, 893 F.2d 370, 373 (D.C. Cir. 1990); *Lewis v. Dept. of Treas.*, No. 20-494, 2021 WL 4290635, at * 5 (D. Md. Sept. 21, 2021); *Barouch v. U.S. Dep't of Just.*, 962 F. Supp. 2d 30, 67 (D.D.C. 2013).[6] The logic of these cases is that, in the absence of a request that follows (and exhausts) the prescribed administrative process, there has not been a "properly framed request" to the agency. *Taylor*, 127 F.3d at 474. I agree with these decisions, and Ms. Ruell does not dispute that she had an obligation to exhaust her remedies. She didn't do so, so her claims can't proceed.

For both her amendment claim and her access claim, SORN specified a procedure for Ms. Ruell to follow. She had to contact Mr. Williams in writing. *See* SORN at 36586. For the amendment claim, she had to "state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record." *Id.*

[6] Unlike amendment claims, the Privacy Act does not set forth an administrative exhaustion process for access claims. *See Taylor*, 127 F.3d at 476; 5 U.S.C. §§ 552a(d)(1). Instead, the exhaustion requirements appear in SORN. The Third Circuit has never determined whether compliance with an agency's regulatory requirements is a jurisdictional prerequisite to bringing an access claim under the Privacy Act. But the Fifth Circuit's reasoning in *Taylor* persuades me that a failure to exhaust administrative remedies as to an access claim does "not constitute a jurisdictional bar to assertion of [the] claim in federal district court." *Taylor*, 127 F.3d at 476. Instead, the jurisprudential exhaustion doctrine applies, and Ms. Ruell is not "entitled to judicial relief for a supposed or threatened injury until the prescribed administrative remedy has been exhausted." *Id.* (quotation omitted). A "court should only excuse a claimant's failure to exhaust administrative remedies in extraordinary circumstances." *Id.* at 477 (same). Ms. Ruell hasn't made an argument about or demonstrated that extraordinary circumstances exist, so I have no basis to excuse the exhaustion obligation.

For the access claim, she had to provide her "full name, address, telephone number, … sign[] … the request[], and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort." *Id.* Ms. Ruell never contacted Mr. Williams for any of her requests.

For her amendment claim, Ms. Ruell emailed Ms. Elias and Ms. Grewal to express concerns that her information was available and unsecured in VIEWS.[7] For her access claim, she contends that she "formally requested to inspect her records located in VIEWS through the US Office of Special Counsel …." (ECF No. 42 at 5.) In both cases, Ms. Ruell elected to pursue a process other than the one that SORN specifies. That was her prerogative, but it means that she did not exhaust her remedies, which dooms her claims.

Ms. Ruell offers several arguments to avoid this outcome, but none saves her. For example, she points out that SORN says that individuals "should" contact Mr. Williams and argues that doing so is therefore optional. SORN at 36586. That's not a reasonable reading. "[S]hould" is "used to indicate obligation, duty, or correctness[.]" *New Oxford American Dictionary*, 1617 (3rd ed. 2010). The VA specified one path for individuals to pursue for an amendment or access claim. It would make no sense for it to specify that path in a non-mandatory way and then leave it to individuals' discretion to pursue a different path.

[7] Ms. Ruell's emails to Ms. Elias and Ms. Grewal were not requests for amendment. There's a different between expressing concern and making a request for amendment.

Ms. Ruell also complains that the VA's prescribed exhaustion process "sounds a little bit ridiculous." (ECF No. 46-1 at 264:2-3.) It doesn't matter, though, if the process is cumbersome or ridiculous. As Oliver Wendell Holmes once noted, "[m]en must turn square corners when they deal with the Government." *Rock Island A. & L.R. Co. v. United States*, 254 U.S. 141, 143 (1920). And where, as here, the Government has attached "formal conditions to its consent to be sued[,] [then] those conditions must be complied with." *Id.*

Ms. Ruell suggests she can avoid the exhaustion requirement because, when she requested OSC to provide her access to her documents in VIEWS, "[a]t no time did OSC or VA indicate that [her] request is not a valid request nor did they ever suggest [she] request to inspect her records located in VIEWS through [Mr. Williams]." (ECF No. 40 at 5.) But Ms. Ruell doesn't point to any law that suggests that VA had a legal obligation to remind Ms. Ruell about her obligations under SORN. The VA had discretion to respond to Ms. Ruell's request to OSC as it saw fit, including by trying to resolve her concerns. That doesn't mean that the VA had to remind her to exhaust her remedies at the same time.

2. Monetary relief claims

The Privacy Act permits individuals to bring a civil action against an agency that violated the Act. Ms. Ruell's claims for damages arise under the Act's "catchall" provision, which authorizes a suit whenever an agency "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual[.]" 5 U.S.C. § 552a(g)(1)(D). Ms. Ruell claims that the VA failed to

comply with various provisions of the Privacy Act, including by (a) disclosing her records without her consent, in violation of Section 552a(b); (b) failing to publish a notice in the Federal Register that includes "the categories of individuals on whom records are maintained in the system" and "the categories of records maintained in the system[,]" in violation of Sections 552a(e)(4)(B)-(C); and (c) failing to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity[,]" in violation of Section 552a(e)(10). The VA is entitled to summary judgment on each of these claims.

a. Unauthorized disclosure claim

Ms. Ruell's claim that the VA violated the Privacy Act by disclosing her records without her consent is the driving force behind this lawsuit. But to prevail, Ms. Ruell "must offer evidence to support a jury's finding of four necessary elements: (1) the information is covered by the Act as a 'record' contained in a 'system of records'; (2) the agency 'disclose[d]' the information; (3) the disclosure had an 'adverse effect' on the plaintiff (an element which separates itself into two components: (a) an adverse effect standing requirement and (b) a causal nexus between the disclosure and the adverse effect); and (4) the disclosure was 'willful or intentional.'" *Quinn v. Stone*, 978 F.2d 126, 131 (3d Cir. 1992). Ms. Ruell bases her claim both on disclosures to Messrs. Rizzo and Olivo and to other VA employees, but none of the claims can prevail.

i. Disclosures to Messrs. Rizzo and Olivo

Ms. Ruell cannot establish that the disclosures of her records to either Mr. Rizzo or Mr. Olivo had an adverse effect on her. When asked if she claims to have suffered any injury due to Mr. Rizzo having accessed, retrieved, or downloaded her information from VIEWS, Ms. Ruell responded: "No." (ECF No. 46-1 at 31:15-19.) Similarly, when asked whether she suffered any injury from Mr. Olivo accessing her information, Ms. Ruell responded: "No, that I know of." (*Id.* at 31:20-24.) These admissions doom her disclosure claims to the extent they arise from the disclosures to Messrs. Rizzo and Olivo.

ii. Disclosures to other VA employees

The Act does not define what it means to "disclose" information. In Ms. Ruell's view, the VA "disclosed" her personal information to every person who had access to VIEWS. While the VA doesn't provide its own proposed construction, its briefing implies that it would limit the term "disclose" to someone who accessed and saw the records. I don't have to resolve that dispute, though, because under either definition of "disclose," there's no evidence that the disclosures were willful or intentional.

The Privacy Act "does not 'make the Government strictly liable for every affirmative or negligent action that might be said technically to violate the Privacy Act's provisions.'" *Laningham v. U.S. Navy*, 813 F.2d 1236, 1242 (D.C. Cir. 1987). Instead, to prevail on her claim for damages, Ms. Ruell must prove that in disclosing her records, the VA acted in a manner that was willful or intentional, which is conduct that is "somewhat greater than

gross negligence." *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 551 (3d Cir. 1989). This standard requires proof that the VA "commit[ed] the act without grounds for believing it to be lawful, or by flagrantly disregarding others' rights under the Act." *Id.* (quoting *Albright v. United States*, 732 F.2d 181, 189 (D.C. Cir. 1984)). In other words, "the violation must be so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham*, 813 F.2d at 1242. Ms. Ruell has not offered evidence that comes close to such a showing.

First, with respect to Ms. Ruell's broader proposed definition of "disclose," there's no evidence that the VA set up VIEWS with a flagrant disregard for the rights of whistleblowers like Ms. Ruell. It built a system that allowed it to designate records "sensitive" to protect that information. The system might have had flaws, and it might have experienced human error, but Ms. Ruell has offered no evidence to suggest that the VA thought it was unlawful, should have thought it was unlawful, or disregarded the rights of those whose privacy needed protection. To the contrary, when Ms. Ruell brought her concerns to OSC, the VA investigated and made changes to the system. That's the opposite of willfulness or intentionality.

Second, with respect to the VA's narrower interpretation of "disclose," the VA admits that eight individuals viewed records pertaining to Ms. Ruell between June 2022[8]

[8] The VA does not have security event logs for events that occurred before June 2022. So, while the VA says it knows of eight people who accessed Ms. Ruell's logs, she says she knows of at least 19. Even if the VA doesn't have full records, it would not be a

and July 18, 2024. However, the VA also submitted evidence that each individual "was tasked with marking her documents sensitive; is an attorney within VA OGC; was assigned to conduct an internal investigation into Ms. Ruell's complaint on behalf of OIT; or is a member of the DTC Security Admin Team tasked with generating the security event log reports" that the VA used to support its Motion For Summary Judgment. (ECF No. 37-15 ¶ 4.) In other words, the VA has evidence that these individuals had "a need for the record in the performance of their duties[,]" making them proper disclosures under the Privacy Act. 5 U.S.C. § 552a(b)(1). Ms. Ruell has not presented any contrary evidence to establish that these facts are in dispute; nor has she offered any evidence or argument to demonstrate that disclosure to these eight individuals was improper under the Act. Because Ms. Ruell cannot satisfy the intentional/willful element of her claim under either theory, she cannot prevail.

b. SORN claim

Ms. Ruell claims that the VA violated Sections 552a(e)(4)(B)-(C) of the Privacy Act by failing to "identify whistleblowers as a category of individuals on whom records are maintained in the system" and by failing "to state that social security numbers are

basis for a finding of spoliation because Ms. Ruell has no evidence that the VA acted in bad faith. The VA followed its document destruction policies in place at a time when no litigation was pending. And, given my ruling on the bad faith/willfulness element of the Privacy Act claims, a finding of spoliation wouldn't matter because no adverse inference would impact that element of Ms. Ruell's claim.

collected and stored in the system." (ECF No. 27 ¶¶ 59-60.) She's wrong, so she can't prevail.

The SORN identifies the categories of individuals who the system covers as "[i]ndividuals who voluntarily provide personal contact information when submitting correspondence or other documents to the Department, including, but not limited to … VA employees[.]" SORN at 36585. Identifying those who correspond with the VA and/or voluntarily provide their contact information is broad enough to capture whistleblowers.

The general description of the VA's systems of records explains that the system "includes the name, address and ***other identifying information*** pertaining to the correspondent[s]" and contains documents "that may contain the names, addresses and ***other identifying information*** of individuals who conduct business with VA[.]" *Id.* at 36584 (emphasis added). It also explains that users can retrieve records using a "social security number … and other unique identifiers belonging to the individual to whom the information pertains." *Id.* at 36586. Taken together, these disclosures in SORN put a reader on notice that the VA would collect and store social security numbers as part of the "other identifying information" it had; otherwise, a user couldn't retrieve records based on that information.

Even if Ms. Ruell could establish a violation in this regard, her claims would still fail because she cannot prove that she suffered any adverse effect from the alleged violations. For each of the harms she alleges—pecuniary or not—Ms. Ruell attributes those harms to

the disclosure of her information, rather than VA's allegedly inadequate SORN. (*See* ECF No. 40 at 20 ("There is a causal nexus between the ***disclosures*** and the adverse effects.") (emphasis added).) There is no evidence in the record to support a claim that she suffered any harm as a result of the VA failing to include this information in SORN.

c. Inadequate safeguards claim

Ms. Ruell claims that the VA violated Section 552a(e)(10) of the Privacy Act because it failed to put a system in place to keep track of and audit users who view, access, or download records in VIEWS that may contain whistleblower communications or PII.[9] The VA admits that "[f]rom 1996 thru June 2018, … there was no capability to track who accessed a particular document or case file" in the VA's prior system of records. (ECF No. 37-10 ¶ 7.) Once it implemented VIEWS, the VA used Salesforce Shield to track when users accessed a case or downloaded a document.[10] The VA started using Splunk in August 2022. Splunk logs the same events—case access, web clicks, and document downloads—but it retains the logs for longer periods of time than the prior system. As a result, the VA has logs from August 2022 until the present.

---

[9] It is not clear whether Ms. Ruell also intends to assert this claim based on what she perceives to be the VA's inadequate procedures to ensure that PII and other confidential information is marked sensitive in VIEWS. To the extent Ms. Ruell intended to raise such a claim, it fails for the same reason as her disclosure claim. That is, even if the VA did not designate some or all her records as "sensitive," she has failed to establish that the VA's alleged violation was willful or intentional.

[10] It is not clear from the record whether the VA ever had the capability of tracking any time a user ***viewed*** a document in VIEWS.

Ms. Ruell offers evidence that calls some of the VA's assertions into question. Specifically, the VA Report dated July 21, 2023—almost a year after the VA switched over to Splunk—reported that VIEWS "does not capture instances where a user simply viewed case information or downloaded files." (ECF No. 42-6 at 14.) The VA also noted that "in light of this auditing limitation, it is unclear how business and system owners are able to accomplish risk mitigations in the form of auditing user activity … ." (*Id.*) Given this evidence, a jury could conclude that the VA did not have an auditing or tracking system in place to identify which users viewed, accessed, or downloaded records containing whistleblower communications or other PII.

However, even if Ms. Ruell could establish that the VA violated the Privacy Act, she has failed to produce any evidence that the alleged lack of auditing software had an adverse effect on her or caused her economic damages. Again, Ms. Ruell contends that all the harm she suffered was a result of the alleged ***disclosure*** of her information (*see* ECF No. 40 at 20), and she has no evidence establishing a causal connection between the lack of auditing software and any harm she claims to have suffered.

3. Claim for criminal penalties

In her claims under the Privacy Act's criminal provisions,[11] Ms. Ruell seeks both to assert a claim and to demand an order directing the U.S. Attorney to investigate or prosecute. Either way, the claim fails.

First, I can't make a U.S. Attorney take up this matter. Private citizens lack "a judicially cognizable interest in the prosecution or nonprosecution of another." *Leeke v. Timmerman*, 454 U.S. 83, 85-86 (1981) (quotation omitted). That means she cannot "take law enforcement into [her] own hands" to enforce this criminal statute. *United States v. Panza*, 381 F. Supp. 1133, 1138 (W.D. Pa. 1974) (citations omitted). Instead, "the United States Attorney is responsible for the prosecution of all criminal cases within his or her district." *United States v. Friedland*, 83 F.3d 1531, 1539 (3d Cir. 1996). And "the decision whether or not to prosecute, and what charge to file or bring before a grand jury, generally rests entirely in his discretion." *United States v. Armstrong*, 517 U.S. 456, 464 (1996).

Second, Ms. Ruell can't pursue a civil claim for a violation of the criminal provisions of the Privacy Act's criminal provisions. "[T]he fact that a federal statute has been violated and some person harmed does not automatically give rise to a private cause of action in favor of that person." *Touche Ross & Co. v. Redington*, 442 U.S. 560, 568 (1979) (quotation omitted). "[T]he general rule is that a private right of action is not maintainable under a

[11] Though Ms. Ruell cites to Section 552a(i)(1) in her Amended Complaint, the language she quotes comes from Section 552(a)(2). Both provisions impose criminal penalties on individuals (as opposed to agencies).

criminal statute." *Am. Postal Workers Union, AFL-CIO, Detroit Loc. v. Indep. Postal Sys. of Am., Inc.*, 481 F.2d 90, 93 (6th Cir. 1973). To determine whether Congress intended to depart from the usual rule, my "analysis must begin with the language of the statute itself." *Touche*, 442 U.S. at 568. Where, as here, "the text of a statute does not provide a cause of action, there ordinarily is no cause of action." *Jaroslawicz v. M&T Bank Corp.*, 962 F.3d 701, 709 (3d Cir. 2020) (quotation omitted).

In trying to discern Congress's intent, the Supreme Court examines a variety of "factors related to the text and structure of the statute in question, including … the explicit creation of a private right of action elsewhere in the same statute. *Wisniewski v. Rodale, Inc.*, 510 F.3d 294, 303 (3d Cir. 2007)). Congress knew how to provide for civil remedies for violations of the Privacy Act because it created a private right of action against agencies that do not comply with it. *See* 5 U.S.C. § 552a(g)(1). The fact that it knew how to create a private right of action and failed to do so for these provisions leads me to conclude that Ms. Ruell has no private right of action under Section 552a(i). While the Third Circuit has yet to rule on this particular issue, at least one Court of Appeals has determined that Section 552a(i) "provides for criminal penalties only, and generates no civil right of action." *Unt v. Aerospace Corp.*, 765 F.2d 1440, 1448 (9th Cir. 1985). Notably, Ms. Ruell did not dispute this issue in her briefing, so I treat it as conceded.

B. Other Claims

Ms. Ruell's remaining substantive claims, under the IGA and the VBHCITA, fail because neither statute provides a private right of action. "Determining whether a statute explicitly provides a private remedy involves a relatively straightforward inquiry. A court must look to the text of the statute to see if it states, by its terms, that a private party may bring suit to enforce it." *Three Rivers Ctr. for Indep. Living v. Hous. Auth. of City of Pittsburgh*, 382 F.3d 412, 420 (3d Cir. 2004). Neither the IGA nor the VBHCITA contains an express statement that a party may sue under it.

There's also no reason to think that Congress embedded an implied right of action in either statute. To determine if Congress created an implied private right of action, courts must answer two questions: "(1) Did Congress intend to create a personal right?; and (2) Did Congress intend to create a private remedy? Only if the answer to both of these questions is 'yes' may a court hold that an implied private right of action exists under a federal statute." *Wisniewski*, 510 F.3d at 301. To answer those questions, courts look at the statute at issue to see if it "contain[s] 'rights-creating' language that focuses on the 'individual protected' rather than 'the person regulated.'" *Id.* (quotation omitted).

Neither the IGA nor the VBHCITA creates a personal right. Section 7 of the IGA provides: "The Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines the disclosure is unavoidable during the course

of the investigation." 5 U.S.C. § 407(b). This provision does not include any rights-creating language, and the provision's focus is on the person regulated—the Inspector General. Thus, there is no implied private cause of action under this provision.[12]

Section 5724 of the VBHCITA requires the VA Secretary to ensure that the VA's Office of Inspector General or a non-VA entity conducts an independent risk analysis in the event of a data breach of sensitive personal information. *See* 38 U.S.C. § 5724(a)(1). If the Secretary determines that a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach, then the statute requires the Secretary to provide credit protection services consistent with accompanying regulations. *See* 38 U.S.C. § 5724(a)(2). Neither of these provisions contains any rights-creating language.

There is also nothing in either statute suggesting that Congress intended to create a private remedy. It does not offer a way for whistleblowers to enforce the IGA. And Congress has taken responsibility for ensuring the Secretary's compliance with the VBHCITA. Depending on the individuals whose information a data breach might cover, the Secretary must submit a report to the Committees on Veterans' Affairs of the Senate and House of Representatives and/or the Committees on Armed Services of the Senate

[12] Other district courts have also determined that plaintiffs do not have a private right of action under other provisions of the IGA. *See, e.g.*, *Brown v. Ulmer*, No. 21-cv-3128, 2022 WL 226878, at *1 (D.D.C. Jan. 21, 2022); *Alford v. Def. Intel. Agency*, No. 10-cv-631, 2011 WL 13349594, at *2 (D.D.C. Oct. 24, 2011); *Johnson v. Rinaldi*, No. 99-cv-170, 2001 WL 677306, at *5 (M.D.N.C. Apr. 13, 2001); *Seba v. Digenova*, No. 86-cv-2838, 1987 WL 9231, at *5 (D.D.C. Mar. 24, 1987).

and the House of Representatives. *See* 38 U.S.C. §§ 5724(c)(1)-(2). Because the statute requires the Secretary to report to Congress in this way, it suggests that Congress did not intend to create a separate remedy for private individuals.[13] Notably, Ms. Ruell has not responded to the VA's arguments about these statutes, so I treat the issue as conceded.

Finally, because Ms. Ruell cannot prevail on any of her claims, she is not entitled to declaratory relief. The Declaratory Judgment Act "does not itself create an independent basis for federal jurisdiction but instead provides a ***remedy*** for controversies otherwise properly within the court's subject matter jurisdiction." *Auto-Owners Ins. Co. v. Stevens & Ricci Inc.*, 835 F.3d 388, 394 (3d Cir. 2016) (citation omitted) (emphasis added). Having resolved the entire controversy between the Parties in favor of the VA, the Act does not provide a basis for relief. Ms. Ruell does not dispute this in her opposition.

IV. CONCLUSION

If Ms. Ruell wants to see her records in VIEWS or wants to amend them in some way, then she must exhaust the administrative procedures set forth in the Privacy Act and SORN before she can seek relief. As for Ms. Ruell's other Privacy Act claims, the VA is entitled to summary judgment on those claims because Ms. Ruell has failed to establish essential elements of her claims for damages and she cannot enforce the Act's criminal provisions. In addition, Ms. Ruell cannot proceed with claims under the Inspector General

[13] Judge Younge reached the same conclusion in a similar case. *See Crandall v. McDonough*, No. 24-cv-626, 2024 WL 4190867, at *5 (E.D. Pa. Sept. 13, 2024).

Act and the VBHCITA because neither statute authorizes an express or implied private cause of action. Finally, because all her claims fail for one reason or another, Ms. Ruell is not entitled to declaratory relief. An appropriate Order follows.

BY THE COURT:

/s/ Joshua D. Wolson
JOSHUA D. WOLSON

November 13, 2024